



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/940,982	08/29/2001	Takashi Endo	NIT-295	5993
24956 7590 03/24/2009 MATTINGLY & MALUR, P.C. 1800 DIAGONAL ROAD SUITE 370 ALEXANDRIA, VA 22314				
EXAMINER				
DAVIS, ZACHARY A				
ART UNIT		PAPER NUMBER		
2437				
MAIL DATE		DELIVERY MODE		
03/24/2009		PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.



# Office Action Summary

## Application No.

09/940,982

## Applicant(s)

ENDO ET AL.

## Examiner

Zachary A. Davis

## Art Unit

2437

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 11 December 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-8, 18, 20-22 and 24-27 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-8, 18, 20-22 and 24-27 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/C)
- 4) ☐ Interview Summary (PTO-413)
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_
- Paper No(s)/Mail Date \_\_\_\_\_



### **DETAILED ACTION**

1. A response was received on 11 December 2008. By this response, Claims 1, 18, and 24-26 have been amended. Claims 19 and 23 have been canceled. New Claim 27 has been added. Claims 1-8, 18, 20-22, and 24-27 are currently pending in the present application.

### ***Response to Arguments***

2. Applicant's arguments with respect to claims 18, 20-23, 25, and 26 have been considered but are moot in view of the new ground(s) of rejection.
3. Applicant's arguments filed 11 December 2008 have been fully considered but they are not persuasive.

Regarding the objection to the specification for failure to provide proper antecedent basis for the claimed subject matter and the rejection of Claims 1-8 under 35 U.S.C. 112, first paragraph, for failure to comply with the written description requirement, Applicant argues that "it is self-evident that the input data D1 does not have a constant Hamming weight" (page 11 of the present response). Applicant generally alleges that "there are at least a case of a 0 [zero] Hamming weight and a case of a Hamming weight that is non-zero, so that the Hamming weight is not constant in the transformation" (page 12 of the present response); however, Applicant cites no evidence in support of this allegation. Applicant also refers to description in the present



specification of Figure 32, noting that “[d]ata of 32 bits is transformed into the same representation of 32 bits” (page 12 of the present response, citing page 69 of the present specification). Applicant further states that the “representation of 32 bits employs all combination of  $2^{32}$ ” (again, page 12 of the present response); however, the Examiner first notes that this statement is generally unclear and also notes that there is nothing in the cited portion of the specification or elsewhere that appears to explicitly support this allegation. Applicant again states that “there are at least a case of Hamming weight of 0 [zero] and a case of Hamming weight of non-zero, so that the Hamming weight is not constant” (page 12 of the present response); however, this does not appear to necessarily follow from the cited portions of the specification, and Applicant has not clearly explained what is relied upon in the specification for support for the limitation of the input data not having a constant Hamming weight. Although Applicant asserts that the analysis relied upon is “taken directly from the specification”, the Examiner fails to appreciate this argument, since the specification is silent as to the Hamming weight of the input data. This is further supported by Applicant’s statement in the present response that the specification makes no reference to the Hamming weight of the input data (see pages 13-14 of the present response, “the rejection refers to page 21 of the present application, which makes no reference to the Hamming weight of the input data”). The Examiner again submits that there is no reference anywhere in the present specification to the Hamming weight of the input data, constant or not. The Examiner again notes that the absence of a positive recitation in the specification is not basis for an exclusion; that is, the fact that the specification does not state that the



Hamming weight of the input data is constant is not sufficient support for the limitation that the Hamming weight of the input data is not constant.

Regarding the rejections of Claims 1-8, 19, and 24 under 35 U.S.C. 103(a) as unpatentable over Applicant admitted prior art in view of Jaffe et al, US Patent 6510518, Applicant first argues that Jaffe teaches away from the limitation in independent Claim 1 of the input data having a non-constant Hamming weight because Jaffe requires a constant Hamming weight representation (pages 13-14 of the present response). However, the Examiner notes the use of the term "representation"; it is again submitted that even though the values are operated on using a constant Hamming weight data representation, at least the logic values that are initially input before the data is converted into the constant Hamming weight representation do not necessarily have a constant Hamming weight (see Jaffe, column 2, lines 57-67, as previously noted, where the representation of data is transformed; note again that this does not necessarily refer to a specific transformation operation, as the portion at column 4, line 55-column 5, line 30 also does not necessarily refer to a specific mapping operation in contrast to Applicant's previous assertions in prior responses; however, the data at base, which is represented using the constant Hamming weight representation, may or may not itself have a constant Hamming weight). In response to this assertion, Applicant argues that the statement "that Jaffe's logic values do not necessarily have a constant Hamming weight does not constitute a statement that Jaffe's logic values do not have a constant Hamming weight" (page 10 of the present response, emphasis in original). However, the Examiner notes that Jaffe specifically refers to "conventional bit representations" in



contrast to “balanced Hamming weight representations” (see Jaffe, column 2, lines 58-60), which at least implies that the conventional representation does NOT have a balanced (i.e. constant) Hamming weight representation, and therefore the input data before being converted to this representation (see column 4, line 55-column 5, line 30, for example, where the logic values for TRUE/1 and FALSE/0 are replaced with analogous constant Hamming weight representations) does not have a constant Hamming weight as required by the claims. The Examiner notes that this differs from the issue of sufficient written description and proper antecedent basis support as discussed above, because while Jaffe **specifically mentions** data representations that are not necessarily constant Hamming weight and other data representations that have constant Hamming weight (as noted above with respect to the obviousness rejection), the present specification, in contrast, is **silent** as to the Hamming weight of the input data. That is, the specification does not mention either way whether the input data does or does not have a constant Hamming weight. The statement that Applicant admits that “there is no limitation placed on some of the data in the system, namely the disturbance data” (see page 11 of the present response, citing pages 3-4 of the previous Office action) was intended to assist in highlighting this distinction, not to “provide the teaching missing” as Applicant alleges (page 11 of the present response).

Further with respect to the rejection of Claim 1 under 35 U.S.C. 103(a), Applicant again argues that the admitted and cited prior art do not disclose disturbance data with a constant Hamming weight and “the transforming of the data is different between the present invention and Jaffe” (page 14 of the present response). In response to



applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Specifically, Applicant argues that Jaffe "does not use disturbance data itself that corresponds to the disturbance data set forth in the present claims" (page 14 of the present response); however, the Examiner notes that the admitted prior art explicitly discloses the use of disturbance data as claimed (see page 21, lines 1-12, which explicitly disclose "data for disturbance" used to transform and then inverse transform the data to be processed). Applicant then argues that "the admitted prior art does not teach the disturbance data employed as set forth in claim 1" but then further contradicts this assertion by stating that the admitted prior art teaches "using data for disturbance" (see page 14 of the present response). It appears that Applicant may have intended the statement "disturbance data employed as set forth" in the claims to assert that the admitted prior art does not disclose that the disturbance data has a constant Hamming weight; however, this was acknowledged in the previous Office actions (see, for example, the rejection of Claim 1 at pages 10-11 of the previous Office action). Applicant asserts that "there is no suggestion in the admitted prior art to make constant the Hamming weight for the disturbance data" and that the admitted prior art "does not provide the necessary teaching" (page 15 of the present response); however, the Examiner again notes that the admitted prior art was not relied upon for a teaching of constant Hamming weight data. Rather, Jaffe was relied upon for the explicit disclosure that data used in



cryptographic processing can be represented using a constant Hamming weight representation (column 4, line 55-column 5, line 30; column 2, lines 56-60), which suggested modifying the admitted prior art apparatus to include constant Hamming weight disturbance data as claimed, as detailed in the previous Office actions.

Regarding amended Claims 18 and 24, and dependent Claims 2-8, Applicant asserts that similar arguments as detailed in reference to Claim 1 apply (see pages 15-16 of the present response); the Examiner notes that these arguments have been addressed above. The Examiner further notes that Applicant has not presented any arguments with respect to dependent Claims 20-22, 25, or 26, nor with respect to new independent Claim 27. 37 CFR 1.111(b) requires that arguments must be presented "pointing out the specific distinctions believed to render the claims, **including any newly presented claims**, patentable over any applied references" (emphasis added); however, because the present response appears to be a *bona fide* attempt to advance the prosecution of the present application, the response has been treated as though it were fully responsive under 37 CFR 1.111.

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

### ***Specification***

4. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction



of the following is required: Claim 1 was previously amended to recite the limitation "wherein said input data D1 does not have a constant Hamming weight". However, the specification appears to be entirely silent as to the Hamming weight of the input data; there does not appear to be any indication as to whether the input data either would or would not have a constant Hamming weight. Therefore, there is not proper antecedent basis for the limitation in the specification. See below regarding the rejection for failure to comply with the written description requirement under 35 U.S.C. 112, first paragraph, for further detail.

***Claim Rejections - 35 USC § 112***

5. The rejection of Claims 18-22 under 35 U.S.C. 112, second paragraph, as indefinite is withdrawn (or moot) in view of the amendments to (or cancellation of) the claims. The rejection of Claims 1-8 under 35 U.S.C. 112, first paragraph, for failure to comply with the written description requirement is maintained as detailed above.

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 1-8 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one



skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Specifically, independent Claim 1 was previously amended to recite the limitation "wherein said input data D1 does not have a constant Hamming weight". There does not appear to be written description of the above claim limitation in the application as filed. The specification appears to be entirely silent as to the Hamming weight of the input data; there is no indication in the present specification whether the input data either would or would not have a constant Hamming weight. It is noted that the absence of a positive recitation in the specification is not basis for an exclusion (i.e. the negative limitation, that the input data does not have constant Hamming weight). See also MPEP § 2173.05(i). Applicant has referred to the disclosure on page 69 of the present response as providing support for the above limitation (see page 12 of the present response); however, there is also nothing in this portion that refers to or mentions the Hamming weight of the input (plain text) data.

Claims 2-8 are rejected due to their dependence on rejected Claim 1.

### ***Claim Rejections - 35 USC § 103***

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.



9. Claims 1-8, 18, 20-22, and 24-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant admitted prior art in view of Jaffe et al, US Patent 6510518.

In reference to Claim 1, Applicant admits as prior art an apparatus including a data transform means transforming input data by using disturbance data to generate transformed data, where the input data does not have constant Hamming weight; a transformed data processing means for carrying out predetermined processing on the transformed data to generate processed transformed data; and a data inverse transform means for carrying out inverse transformation processing on the processed transformed data using processed disturbance data to generate processed data (see page 21, lines 1-12 of the present application; note, there is no limitation placed on the disturbance data). However, Applicant admits that such prior art does not explicitly disclose that the disturbance data and the processed disturbance data have a constant Hamming weight.

Jaffe discloses that data used in cryptographic processing can be represented using a constant Hamming weight representation but that input data before the Hamming weight representation does not necessarily have constant Hamming weight (column 4, line 55-column 5, line 30; see also column 2, lines 56-60; however, the data that is represented by a constant Hamming weight representation does not necessarily, and does not likely, have a constant Hamming weight itself). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of the prior art to include constant Hamming weight data, in order minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48).



In reference to Claim 2, Applicant admits that the prior art further discloses that the processed disturbance data can be generated by carrying out the predetermined processing on the disturbance data (page 21, lines 6-8 of the present application; see also prior art Figure 4).

In reference to Claim 3, Jaffe further discloses that each bit has a logic value of 1 or 0 at a probability of 50% (see the table at column 9, noting the representations  $s_8$ ; see also column 8, lines 41-45, and column 5, lines 12-18).

In reference to Claim 4, Applicant admits that the prior art further discloses generating processed disturbance data by carrying out the predetermined processing on the disturbance data (page 21, lines 6-8 of the present application; see also prior art Figure 4, and Jaffe, column 4, line 55-column 5, line 30).

In reference to Claim 5, Applicant further admits and Jaffe further discloses a disturbance data storage means, disturbance data select means, and that processing is carried out on the disturbance data in order to generate the processed disturbance data (page 21, lines 6-8 of the present application, and prior art Figure 4; Jaffe, column 16, lines 15-32).

In reference to Claim 6, Jaffe further discloses means for generating random numbers each having a Hamming weight equal to half the numbers of bits include in the random number (column 7, lines 62-64; see Figures 1 and 4; see also column 5, lines 12-18), means for inverting bits of data (column 8, lines 41-45; Figure 1, step 150; Figure 4, step 450), and means for concatenating a random number with data output by the means for inverting (Figure 1, steps 110-120; Figure 4, steps 410-420).



In reference to Claim 7, Jaffe further discloses a random number generation means (column 7, lines 62-64), a Hamming weight computation means (see Figure 1; column 8, lines 25-29 and 46-65), a Hamming weight examination means (see Figure 1; column 8, lines 25-29 and 46-65), and a constant Hamming weight assurance means (see column 4, line 55-column 5, line 30, where the representations guarantee a constant Hamming weight).

In reference to Claim 8, Jaffe further discloses random number generation means to generate partial random numbers with uniform constant Hamming weights and bit count each equal to a fraction of a final random number (Figure 1, step 115; Figure 4, step 415); means to generate random numbers until a sum of bit counts is equal to the final bit count (column 7, lines 62-64); and means for concatenating the partial random numbers (Figure 1, steps 110-120; Figure 4, steps 410-420).

In reference to Claim 18, Applicant admits as prior art an apparatus including a processor (see prior art Figure 2, CPU 201, coprocessor 202; page 2, line 14-page 3, line 5 of the present application), a storage (Figure 2, storage device 204; page 2, lines 14-17; page 3, line 8—page 4, line 2) arranged to store programs (Figure 2, program memory 205; page 3, line 12) and data (Figure 2, data memory 206; page 3, lines 12-14), and a data bus interconnecting the processor and storage (Figure 2, bus 203; page 3, lines 5-7). Applicant further admits that the processor is arranged to transform input data into first transformed data with first disturbance data, process the first transformed data with a first operation, generate second transformed data, process the first



disturbance data with the first operation, generate second disturbance data, and inverse-transform the second transformed data into processed data with the second disturbance data (see page 21, lines 1-12 of the present application). However, Applicant additionally admits that such prior art does not explicitly disclose that the disturbance data has a constant or target Hamming weight, and in particular, the prior art does not explicitly disclose that each bit in the disturbance data has a logic value of 0 or 1 at a probability of 50%.

Jaffe discloses that data used in cryptographic processing can be represented using a constant Hamming weight representation (column 4, line 55-column 5, line 30; see also column 2, lines 56-60). More specifically, Jaffe discloses that each bit has a logic value of 1 or 0 at a probability of 50% (see the table at column 9, noting the representations  $s_8$ ; see also column 8, lines 41-45, and column 5, lines 12-18). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of the prior art to include constant Hamming weight data, where the disturbance data has appearance probabilities of 50% for either 0 or 1 for each bit, in order minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48).

Further, neither Applicant nor Jaffe explicitly discloses that the first disturbance data of  $n$  bits is generated by concatenating a predetermined number of  $m$ -bit random numbers. Official notice is taken that it is well known that, in order to generate long random numbers, a series of shorter random numbers can be generated and concatenated together. In particular, if one only has access to a device that can



generate at most  $m$  bit long random numbers, and if one needed a longer,  $n$  bit random number, then one could simply generate a plurality of  $m$  bit random numbers and concatenate sufficient of them together until the new string was  $n$  bits long. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the generation of the  $n$  bit first disturbance data by concatenating a predetermined number of  $m$  bit random numbers, in order to realize the predictable result of the generation of a longer random number of the desired length of  $n$  bits, using available hardware and/or algorithms.

In reference to Claim 20, further Official notice is taken that it is well known to collect data in a table. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a table for the  $m$  bit random numbers in order to realize the predictable result of easier and more organized access to any of the  $m$  bit numbers that were desired to be used.

In reference to Claim 21, Applicant further admits and transforming data by means of an XOR operation (or an addition or transform operation) (see pages 8 and 9 of the present application, noting Expressions 3, 4, 5, 7, 9, and 10, in particular).

In reference to Claim 22, Applicant further admits performing a rotate operation, a shift operation, or a bit permutation operation (see pages 8 and 9 of the present application, noting Expressions 2, 6, and 8 in particular).

In reference to Claim 24, Applicant admits as prior art an apparatus including a processor (see prior art Figure 2, CPU 201, coprocessor 202; page 2, line 14-page 3,



line 5 of the present application), a storage (Figure 2, storage device 204; page 2, lines 14-17; page 3, line 8—page 4, line 2) arranged to store programs (Figure 2, program memory 205; page 3, line 12) and data (Figure 2, data memory 206; page 3, lines 12-14), and a data bus interconnecting the processor and storage (Figure 2, bus 203; page 3, lines 5-7). Applicant further admits that the processor is arranged to transform input data into first transformed data with first disturbance data, process the first transformed data with a first operation, generate second transformed data, process the first disturbance data with the first operation, generate second disturbance data, and inverse-transform the second transformed data into processed data with the second disturbance data (see page 21, lines 1-12 of the present application). However, Applicant additionally admits that such prior art does not explicitly disclose that the disturbance data has a constant or target Hamming weight, and in particular, the prior art does not explicitly disclose that each bit in the disturbance data has a logic value of 0 or 1 at a probability of 50%.

Jaffe discloses that data used in cryptographic processing can be represented using a constant Hamming weight representation (column 4, line 55—column 5, line 30; see also column 2, lines 56-60). More specifically, Jaffe discloses that each bit has a logic value of 1 or 0 at a probability of 50% (see the table at column 9, noting the representations  $s_8$ ; see also column 8, lines 41-45, and column 5, lines 12-18). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of the prior art to include constant Hamming weight data, where the disturbance data has appearance probabilities of 50%



for either 0 or 1 for each bit, in order minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48).

In reference to Claim 25, Applicant further admits transforming data by means of an XOR operation (or an addition or transform operation) (see pages 8 and 9 of the present application, noting Expressions 3, 4, 5, 7, 9, and 10, in particular).

In reference to Claim 26, Applicant further admits performing a rotate operation, a shift operation, or a bit permutation operation (see pages 8 and 9 of the present application, noting Expressions 2, 6, and 8 in particular).

In reference to Claim 27, Applicant admits as prior art an apparatus including a data transform means transforming input data by using disturbance data to generate transformed data, a transformed data processing means for carrying out predetermined processing on the transformed data to generate processed transformed data, and a data inverse transform means for carrying out inverse transformation processing on the processed transformed data using processed disturbance data to generate processed data (see page 21, lines 1-12 of the present application). However, Applicant admits that such prior art does not explicitly disclose that the disturbance data and the processed disturbance data have a constant Hamming weight.

Jaffe discloses that data used in cryptographic processing can be represented using a constant Hamming weight representation (column 4, line 55-column 5, line 30; see also column 2, lines 56-60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of the



prior art to include constant Hamming weight data, in order minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48).

### ***Conclusion***

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-



3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ZAD/  
Examiner, Art Unit 2437

/Emmanuel L. Moise/  
Supervisory Patent Examiner, Art  
Unit 2437